Junio 2017



La Revista del Líder de Tecnología



SOLUCIONES de Colaboración y Teletrabajo

IT COMO SERVICIO un Proyecto Empresarial

RADAR de Riesgo Tecnológico

ISSN 13908251







3.000 ejemplares



Notas del Editor



La seguridad corporativa en la era digital

La nueva era digital junto a la dependencia de la tecnología y uso de las TIC en los negocios suponen una amenaza para las actividades de las empresas. Los intentos de fraude y ataques no paran y cuando logran su objetivo, frecuentemente, se debe al desconocimiento de los usuarios de políticas claras a seguir.

La necesidad de capacitación y concienciación en seguridad es hoy una pieza vital para garantizar la continuidad de las actividades de todo negocio.

Hemos visto en varias oportunidades que temas como la Seguridad de la Información entre otras tendencias en la nueva era de los Negocios Digitales, han sido abordados de una forma teórica. Sin embargo, es necesario tener la perspectiva de los usuarios: cómo empoderados en su nuevo rol gestionan en la práctica las nuevas corrientes tecnológicas y las oportunidades que las empresas tienen para definir acciones, procesos, en un momento en que las compañías están adoptando modelos digitales, que va más allá de la sola compra de herramientas.

El desarrollo de los temas propuestos en esta edición permitirá a los equipos ejecutivos tomar decisiones de negocios. Hemos considerado las opiniones de proveedores, usuarios y firmas consultoras, nos proporcionarán un panorama lo más cercano a la realidad del mercado ecuatoriano.

Muchas gracias a nuestros colaboradores e invitamos a nuevos profesionales a compartir sus experiencias y buenas prácticas de IT para futuras ediciones.


Janeth Martínez


Anavela Herrera


*Si eres líder de tecnología y quieres recibir de cortesía la revista **IT ahora**, escríbenos a: info@itahora.com*
Comentarios o sugerencias escríbanos a redaccion1@itahora.com

***IT Ahora** es una revista ecuatoriana que en cumplimiento con los requisitos promulgados por la nueva Ley de Comunicación vigente en la República del Ecuador, pone en conocimiento público a través de la revista y nuestra pagina web www.itahora.com nuestra políticas editoriales e informativas como visión y misión. Somos una revista de circulación dirigida a líderes de IT que se distribuye a nivel nacional.*

Directora
Janeth Martínez
janeth.martinez@itahora.com

Editora
Anavela Herrera
anavela.herrera@itahora.com

Redacción
Karen González
redaccion1@itahora.com

Relaciones Públicas
Cora Hervás
comunicaciones@innovacom-ec.com

Diseño y Diagramación
Tinta Diseño Visual

Fotografía
José Alvarado
Xavier Caivinagua

Corrección de estilo
Innovacom

Contadora
Elizabeth Erazo

Impresión
Nueva imprenta Don Bosco

Una Producción de
Innovacom
Integrando comunicaciones

Dirección
Av. de la Prensa N49 - 98
y Río Curaray.

Teléfonos
(593.2) 2247 910 / (593.2) 2273 939

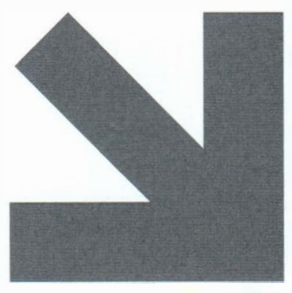


SUMARIO

Identifica nuestros contenidos bajo esta iconografía

O OPINIÓN | I INFORMATIVO | P PUBLICIDAD

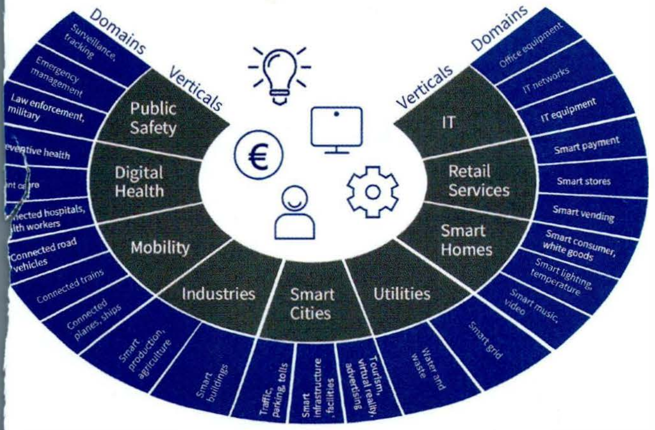












www.itahora.com

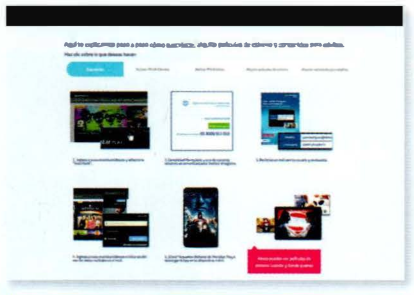
SÍGUENOS EN: @Itahora

/ Revista de Tecnologia online del Ecuador

www.itahora.com

Nuevos servicios de entretenimiento para el usuario

Los servicios de telefónica presentan nuevos servicios de entretenimiento para sus clientes. Movistar presentó en el país Movistar Play, un servicio de video online (streaming) que presenta películas, series, documentales y contenidos infantiles. A este contenido se puede acceder desde cualquier dispositivo móvil, como celulares, Tablet, PC o televisión. Además, presenta Studio+, un contenido Premium exclusivo de video para Smartphone, de corta duración. Se puede encontrar series de acción, thriller, aventura, romance y más. No consumen datos.









Claro, también, presentó dos plataformas de entretenimiento: Claro video y Claro música. A estas plataformas se puede acceder desde cualquier dispositivo que esté conectado a internet. Los contenidos de Claro video están disponibles en calidad de alta definición. La empresa recalcó que Claro música tiene como objetivo apoyar a la industria musical ecuatoriana estrenando sus sencillos como contenido exclusivo de la plataforma sin consumo de datos.

Para su instalación, estos servicios se encuentran ya disponibles en el Play Store y el App Store.

Sony Mobile presenta el nuevo smartphone: **Xperia L1**



Sony Mobile Communications dio a conocer el Xperia L1. Este smartphone tiene una apariencia sencilla, cuenta con una pantalla HD de 5.5" y 256 GB de memoria expandible. Adicionalmente, tiene incorporado el "Smart Cleaner" que trabaja en segundo plano eliminando automáticamente procesos no utilizados y datos de caché.

El Xperia L1 incluye funciones de interés para el usuario: el motor "Xperia Actions" de Sony Mobile que adapta de forma receptiva la configuración y la funcionalidad del dispositivo al entorno. El modo "Buenas noches" pondrá automáticamente el dispositivo en la configuración "No molestar", de esta manera, disminuirá el brillo de la pantalla y garantizará que no existan interrupciones mientras se carga. El "Xperia Tips" (Consejos), que se introdujo en 2016, funciona como un asistente personal que se ajusta a las preferencias del usuario para brindar consejos pertinentes y oportunos en pantalla que ayudan a aprovechar todas las funcionalidades del dispositivo.

FounderList generó un diálogo entre inversionistas y emprendedores



► *Thierry Benoit, consultor en Humboldt Management, José Villareal, co-fundador de 593 Capital Partners, Ernesto Kruger, Fundador de Kruger Corporation.*

Quito fue elegido como la segunda sede para el evento creado por FounderList: El Off The Record de la Inversión en Startups. Al encuentro asistieron alrededor de 250 personas para hablar de inversión de riesgo en compañías de etapa temprana. Entre los asistentes se encontraban inversionistas como: Ernesto Kruger, Fundador de Kruger Corporation, Guillermo Poveda, director Ejecutivo de Kruger Labs, José Villareal, co-fundador de 593 Capital Partners, Thierry Benoit, propietario de Humbolt Management.

Adicionalmente, asistieron emprendedores como: Martín Jara, co-fundador de Yaesta.com, Juan José Lasso, propietario de Lassi´s, especería artesanal, Adrián Armijos, CEO The Wawa, Pedro Varas, CEO & Co-Fundador de FounderList.

La organización estuvo a cargo de Kruger Labs, empresa que consiguió el apoyo de 15 importantes organizaciones del ecosistema de emprendimiento entre ellas Redes de ángeles, Fondos de Inversión, Incubadoras/Aceleradoras, organizaciones gubernamentales, Universidades y Coworkings.

Entre las lecciones que dejó el evento se destacaron las siguientes: los emprendedores deben enfocarse en tener un negocio llamativo para que los inversionistas vengan a buscarlos, la meta de una startup no puede ser, únicamente, levantar dinero. "No es real la hipótesis de: tengo una idea y vale USD $100.000, invierte en mi compañía" recalcó Guillermo Poveda.

Adrián Armijos comentó que los emprendedores deben buscar las otras cosas que pueden aportar los inversionistas, no solo el dinero. "Es importante las conexiones y las áreas en las que necesiten expertos".

Comstor organizó sesión informativa

Comstor junto a socios de negocio realizó una sesión informativa sobre herramientas Cisco Meraki y Advanced Threat Solutions. Durante la presentación se demostró el uso de soluciones Cisco.

Jorge López, gerente de distribución para Latinoamérica de Cisco-Meraki, señala que la consola de administración de red Meraki es intuitiva y sencilla de gestionar. "Lo hace a través de una Dashboard desde donde se visualiza y recopila la información del comportamiento de red de las organizaciones".

Los beneficios para la industria es la simplicidad al obtener un reporte completo de los dispositivos y aplicaciones utilizados por los usuarios que pasan por la red. López señala que desde el dashboard es posible analizar el tráfico interno, el de terceros, visualizar el porcentaje y tipo de información a la que acceden los usuarios, el tipo de aplicaciones que pasan por la red. Además, el sistema permite gestionar y aplicar políticas de acceso individuales o por grupo para restringir acceso a ciertas aplicaciones, tráfico no deseo o aplicar horarios de consumo de uso de aplicaciones e iniciar un control granular de acceso a la red.

La solución de Cisco Meraki se implementa en clientes que tienen una red o están iniciándola, es aplicable para una oficina pequeña o múltiples localidades, y la visualización y monitoreo se realiza de forma centralizada.

López mencionó que la solución es flexible y crece también bajo demanda, se accede a través de un access point y aumenta según las necesidades de crecimiento y bajo demanda.



► *Augusto Galindo, ingeniero de Sistemas de Seguridad; Gabriela Robalino, gerente Comercial; Alex Carrera, product Manager, de Comstor Ecuador y Jorge López, gerente de distribución para Latinoamérica de Cisco-Meraki*

"**La regulación** debe flexibilizarse para mejorar la competitividad"

Las regulaciones deben adaptarse al futuro pero también a las políticas de fomento de inversión e infraestructura que tiene el gobierno en el Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2020, dice Víctor García, director Regulatorio de Claro Ecuador. Y en esa medida cree necesario regular sobre principios y no sobre la base de funcionamiento de servicios, "al regular sobre principios se puede hablar de seguridad jurídica y abrir paso a la inversión y a la dinamización del mercado", dice.



► *Víctor García, director Regulatorio de Claro.*

Sugiere se revise las directrices de procedimientos sancionatorios de manera que no sean factores que ahuyenten la inversión y "dejar la regulación en materia de calidad de servicios a un atributo competitivo para que los usuarios debidamente informados seleccionen el operador".

En la Ley Orgánica de Telecomunicaciones se establece que las operadoras tendrán cargas tributarias según los niveles de participación del mercado. Para García, el marco regulatorio debería definir el tipo de mercado, porque hay nuevos servicios, señala que los tradicionales mercados fijos y móviles quedaron obsoletos pues se han diversificado. Por ejemplo, los servicios de telefonía fija cambiaron, ahora se utiliza el servicio a través de internet; y aplicaciones de mensajería permiten hablar por teléfono. Existen otro tipo de proveedores de servicios no tradicionales en el mercado que proveen servicios remotamente y cuyas operaciones no están en el país, por lo tanto no invierten en infraestructura en Ecuador.

El director regulatorio de Claro señala que considerando estos casos, la regulación debe cambiar de visión, es decir con el desarrollo tecnológico no hay un operador dominante.

"No estamos en contra de avances tecnológicos e innovación pero no puede ser que los operadores tradicionales que tienen la responsabilidad de desplegar la infraestructura e invertir en el país tengan cargas tan asimétricas con respecto a otros operadores".

Finalmente, García dijo que la regulación debe flexibilizarse para mejorar la competitividad, estimular políticas al fomento de la industria local para contribuir al país.

Evento de seguridad y banca se realizó en Quito



► *Showroom durante el Security Bank & Government.*

La tercera edición del Security Bank & Government se desarrolló en Quito y convocó a los profesionales con nivel de decisión y especialistas de seguridad, y tecnología para tratar sobre tendencias, estrategias, herramientas, normas internacionales, estadísticas, relacionado a la seguridad de la información del sector financiero. Algunos temas fueron abordados a través de exposiciones de expertos, entre los temas tratados: Seguridad física, bancaria, riesgos en canales electrónicos, seguridad operacional, gobierno corporativo, etc.

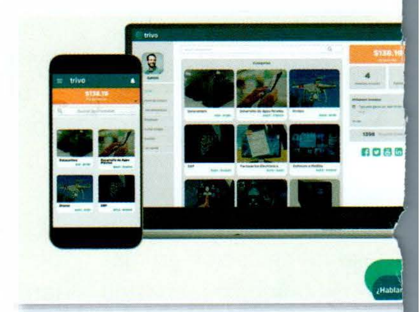
En el showroom participaron expositores como Eset, Easy Solution, entre otros.

Trivo es una aplicación para generar ingresos adicionales

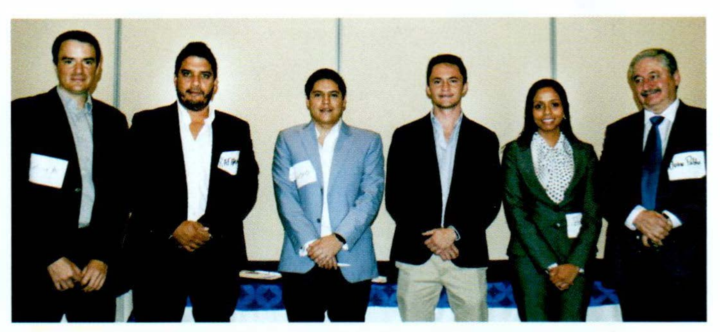
Trivo es una aplicación ecuatoriana que permite al usuario generar ingresos extras por medio de la conexión de clientes con las principales empresas de tecnología del país. Lo que se requiere es conectar las necesidades de una o varias personas de su círculo social y esperar que la empresa cierre el negocio para obtener una comisión por venta. Esta aplicación se presenta como un trabajo extra para las personas, de esta manera, no deberán dejar de realizar sus actividades diarias.

Para utilizarla no se requiere ser un experto en el producto o servicio que se vende, únicamente, hay que estar al tanto de las necesidades de los relacionados. Actualmente, 17 empresas forman parte de la plataforma y esperan que aumente en los próximos meses.

Trivo tiene en el mercado 3 meses, cuenta con 4.446 usuarios y se espera que, al finalizar el primer año de operación, este número ascienda a 15.000 usuarios.



Seidor es el socio estratégico de El Ordeño



► *De Seidor: César Andrade, gerente Comercial, Rafael Saravia, director Regional de Operaciones, Álvaro Celleri, Business Controller de El Ordeño, Juan Pablo Grijalva, Organizational Development de El Ordeño, Jessica Palomino, gerente de Proyecto de Seidor, Juan Pablo Grijalva Cobo, CEO de El Ordeño.*

Seidor, empresa proveedora de soluciones de software y consultoría en gestión y servicios TIC, implementó el ERP SAP S/4 HANA en El Ordeño, empresa industrial de productos lácteos, con la proyección para la transformación digital.

César Andrade, gerente Comercial de Seidor, comentó que la empresa trabajará como aliado estratégico de El Ordeño. Un grupo de consultores estará monitoreando y se mantendrá pendiente de todos los requerimientos que su cliente necesite.

HPE abrió bodega en Cuenca

Hewlett Packard Enterprise, HPE, empresa de tecnología dedicada a la comercialización de servidores, almacenamiento, networking y servicios, abrió en la ciudad de Cuenca una bodega de repuestos.
Desde esta bodega se brindará a los clientes corporativos respuestas inmediatas en la entrega de partes, repuestos y un recurso en sitio del fabricante.



► *En la Foto de izquierda a derecha: Johnny Vivar, Teritory Account Manager; Gem Rivadeneira, Managing & Director and Country Manager Enterprise Group Ecuador; Edgar Barahona, SMB & Channel Manager; Francisco Torres, Data Center Infrastructure; Pablo Maldonado, Service Line Manager y Luis Bravo, ejecutivo de HPE.*

Le decisión de abrir este nuevo centro de acopio se debe a que Cuenca es un mercado importante por su tamaño, número de clientes en el austro y la zona sur del país.

Con este centro de acopio los clientes y canales de HPE y las empresas que buscan optimizar recursos y mejorar su infraestructura se beneficiaran con la entrega rápida de productos y acompañamiento necesario en todo el ecosistema de tecnología.

Los tiempos de espera de los canales en la atención posventa, así como la satisfacción a requerimientos se reducirán en al menos 24 horas. El compromiso de HPE es solventar una necesidad en seis horas desde el momento del requerimiento de partes y piezas.

Los desafíos para ir a 5G

5G estará definido como estándar a finales del 2019, y se prevé que para el 2020 ya se lo utilice. Sebastián Cabello, director Regional para América Latina de GSMA, señaló que hay procesos previos que cumplir. Entre ellos, menciona la limpieza del espectro para habilitar su disponibilidad para las operadoras, entrega y mayor uso del espectro en 4G. El espectro, según Cabellos, es el oxígeno de la industria móvil y no tiene sentido que se lo maneje de manera restrictiva.

Para 5G son necesarias bandas de frecuencia altas que requieren una gran cantidad de antenas, por ejemplo, bandas de 24.25 - 27.5 GHz banda pionera para 5G en Europa; 28 GHz a ser utilizada por EE.UU, Corea y Japón; 31.8 - 33.4 GHz, etc.

En Ecuador, las empresas de telefonía móvil están invirtiendo para mejorar servicios, además, el país cuenta con una buena cobertura, un crecimiento de antenas, alfabetización digital. Lo que hace falta trabajar, dice Cabello, es en un marco regulatorio menos restrictivo que atraiga la inversión y niveles competitivos con empresas locales.

"Hace falta educar a los reguladores para que entiendan el nuevo contexto tecnológico, que contemple un nuevo marco regulatorio con los nuevos servicios de convergencia. No se trata de prohibir los nuevos servicios sino encuadrar a la regulación para que comprenda lo nuevo".



► *Sebastián Cabello, director Regional para América Latina de GSMA*

Ecuador presente en el **SAPPHIRE**



► *En la foto los representantes de AUSIA, junto a Bill McDermott, CEO de SAP.*

En el evento anual de SAP denominado SAPPHIRE realizado en Orlando se anunció la plataforma SAP Leonardo, como una tecnología de innovación para la transformación de los negocios.

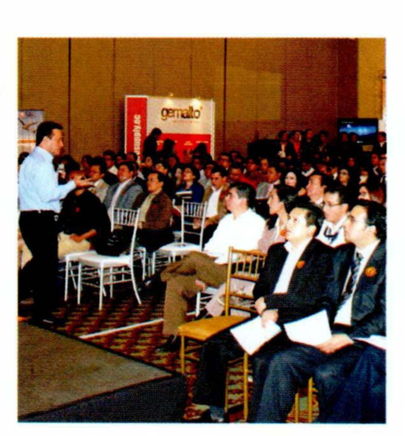
Esta plataforma de negocios se apoya en el Internet de las Cosas IoT y busca inteligentemente conectar a personas, cosas y negocios. Se considera a Leonardo como el mayor movimiento tecnológico después del lanzamiento de SAP Hana.

Dentro del evento SAPPHIRE se desarrolló la reunión anual de la Asociación de Usuarios SAP de Iberoamérica (AUSIA), en la que participaron miembros de ASUG Ecuador. En esta cita se compartieron experiencias y definieron estrategias.

La seguridad en la transformación digital, prioridad en el **Infosecurity 2017**

ISEC, empresa especializada en seguridad de la información, realizó el Infosecurity 2017, un encuentro que reúne a los gerentes de IT y oficiales de seguridad de la información de las empresas, para dialogar sobre las tendencias, riesgos y soluciones para precautelar la información de la empresa.

En este año, el encuentro contó con la participación de empresas como Watchguard, ESET, Prosupply, ZY Proyect, Thales, entre otras. El evento cerró con un panel de expertos en seguridad informática, organizado por IT ahora, donde se discutió sobre los nuevos negocios digitales: "¿Qué competencias se requieren para enfrentar los nuevos riesgos digitales de la empresa?" En el mismo, participaron expertos en seguridad como Fernanda Rodríguez, presidenta de ISACA Quito, Robert Chávez, gerente de Consultoría de Riesgos de Deloitte, José Adrián Pino, jefe de Seguridad de Información de Pronaca. De acuerdo a este conversatorio, la seguridad de la información debe ser parte de la planificación estratégica de la organización.



► *Al Infosecurity 2017 asistieron alrededor de 267 participantes.*

Cloud de SAP cuida la seguridad mientras que los clientes se focalizan en el negocio

Las aplicaciones cloud están disponibles a lo largo y ancho de todo el mundo.

Las funcionalidades son múltiples y asequibles para pequeños y medianos negocios en Ecuador. Las facilidades en los modelos de cloud como Software as a Service, SaaS permite escalabilidad en recursos de cómputo, ahorro y optimización de costos.

SaaS como un modelo de entrega de aplicaciones a través del internet no requiere comprar, instalar, mantener ni actualizar hardware o software porque el proveedor brinda todas las facilidades para e l uso y acceso al software.

En este escenario, las políticas de seguridad implantadas en los data centers de SAP donde se alojan estas aplicaciones cumplen las políticas de seguridad con los más altos estándares de seguridad informática que garantiza un ambiente seguro en el manejo de información de la organización.

Para que un proveedor SaaS garantice la seguridad de los datos debe disponer de un programa de seguridad amplio y multifacético.

Las aplicaciones cloud de SAP tienen un enfoque holístico de la seguridad de la información, implementando sus defensas en todos los puntos de contacto tanto físicos como lógicos. Estas defensas se distribuyen por las siguientes capas:



Capa 1:	Sitio físico
Capa 2:	Base de datos
Capa 3:	Middleware
Capa 4:	Aplicaciones
Capa 5:	Redes y comunicaciones

A medida que el software malicioso, el robo de identidad y los ataques a los data centers, amenazan la informática actual. Proteger los datos corporativos sensibles nunca ha sido más imperativo.

La capacidad de SAP para ofrecer aplicaciones asequibles, configurables y seguras le convierte en El líder de la industria.



César Andrade, gerente Comercial Seidor Ecuador.



Competencias para un CIO en la transformación digital



► *En una conversación informal, Javier Hidalgo, vicepresidente de Tecnología de Produbanco -Grupo Promerica, Rubén Recalde, Cio de Pronaca, Juan Cabrera, IT Plant Manager de General Motors Ecuador, hablaron de la experiencia de vivir día a día los retos de ser un CIO.*

El encuentro de CIO y líderes de IT, CIONET, realizó su primer evento del año 2017 en Ecuador. En el conversatorio denominado "Las claves y competencias para convertir a un CIO en admirable", participaron Xavier Ordeñana, decano asociado y profesor de la ESPAE, Daniela Andretta, directora de Korn Ferry en Ecuador, Javier Hidalgo, vicepresidente de Tecnología de Produbanco-Grupo Promerica.

Daniela Andretta, directora de Korn Ferry en Ecuador habló de las nuevas habilidades que se exigen con las tendencias de transformación digital, a la que se incorpora nuevos conceptos como el de sostenibilidad digital que exige nuevas habilidades productivas en ese entorno. "El talento digital debería tener entre otras cosas agilidad mental, pensamiento crítico, confort con lo complejo, la predisposición para enfrentar situaciones cambiantes, manejar y enfrentar disconformidades".

Andretta indicó que todas las empresas irán hacia la transformación digital y es preciso retener y desarrollar el mejor talento para las empresas. "Las capacidades críticas que debe tener el CIO son las mismas para el CMO, CDO, COO: agilidad, conectividad, transparencia, alineación y empoderamiento, pero sobre todo ideas propositivas de rentabilidad del negocio".

Para Javier Hidalgo, Vicepresidente de Tecnología de Produbanco, los CIO deben reinventarse para trabajar en la transformación digital y comprender las nuevas habilidades competitivas en este cambio.

En el caso de la banca, las estadísticas advierten que para el 2020, el 75% de los clientes no asistirán físicamente a un banco para realizar sus transacciones. Hidalgo mencionó algunos datos de interés del 2016 relacionados con la participación en la transformación digital de los distintos niveles con cargos de gerencia o denominados ejecutivos de nivel C+.

Liderazgo en la transformación digital

34%	los CMO lideran las iniciativas de transformación digital.
27%	los CEO.
19%	los CIO o CTO.
15%	los CDO.

Fuente Altimeter Group



Los datos ayudan a encontrar respuestas

BI Solutions realizó el taller sobre Analítica Avanzada, en el que se expuso sobre rentabilización de la información, experiencias y demostraciones del Software Tableau como una herramienta para optimizar la cadena de suministros, generar presupuestos con analítica predictiva y manejo de grandes volúmenes de datos.

Hugo Vera, gerente de BI Solutions habló sobre analítica avanzada y la creación de modelos predictivos de análisis de tendencias y análisis de clúster. Además, realizó una demo para el análisis de puntos de venta. Vera, indicó que para generar modelos predictivos es necesario un histórico donde aprender de la data, también sostuvo que hay un sinnúmero de oportunidades con analítica predictiva para mejorar distintos procesos de una organización, por ejemplo, inventarios.



► *Guilherme Duarte, evangelizador de analítica; Claudia Mihkelson, gerente de Ventas para Latinoamérica; Alvaro Lira, gerente de Cuentas Estratégicas de Tableau.*

La información es la nueva moneda de la civilización aunque es importante tenerla, es más importante saber extraerlos y para ello, es necesario una plataforma de análisis. La parte más importante de una plataforma de datos es la facilidad de uso y la capacidad de conectar a los datos desde cualquier lugar.

Los datos son considerados como el nuevo oro en la era digital, según IDC en una proyección al 2020 existirán alrededor de 4.4 zetabytes de datos a nivel mundial, su sistematización permitirá la toma de decisiones con mejor y mayor exactitud a nivel empresarial.

Aunque, los seres humanos tienen capacidades de analítica desde el mismo momento en que toman una decisión, aún existe una desconexión sobre cómo y para qué utilizar los datos. Guilherme Duarte, evangelizador de analítica de Tableau, señala que el análisis de datos no es un tema complejo o solo para expertos, la única diferencia son los niveles de conocimiento. "Estamos frente a una nueva economía donde la información es la nueva moneda de la civilización, además de tener la información se requiere saber extraer el conocimiento con una plataforma de análisis".

Para Duarte, los datos públicos o privados tienen la misma importancia para las organizaciones porque los datos ayudan a encontrar respuestas. Ejemplificó, que es posible evitar crisis abasteciéndose de información no estructurada y pública de las redes sociales y actuar con estrategias inmediatas.

Tableau es una herramienta dirigida al usuario de negocio con el soporte del área de tecnología. Claudia Mihkelson, gerente de Ventas de Tableau para Latinoamérica, señala que la tarea del CIO es preocuparse de la gobernabilidad, normatividad de los datos y unificar criterios sobre el uso de los mismos. La función del CIO es determinar la arquitectura, seguridad, la calidad de la información, gobernabilidad, determinar el tipo de datos que se utilizan y para qué, es decir las funcionalidades estarán administradas por el área de tecnología. Con herramientas de fácil uso, cada área de negocio finanzas, ventas, logística, etc., según sus necesidades y conocimiento analiza los datos que son de su interés y propone una estrategia.

Los retos de la seguridad en

IT ahora, recoge la visión de tres ejecutivos con experiencia, conocedores de Seguridad de la Información, quienes nos acercan su visión sobre las empresas ecuatorianas, nuevas amenazas y las competencias necesarias del gestor de seguridad dentro del nuevo escenario del negocio digital.



► *María Fernanada Rodríguez, presidenta de isaca capítulo Quito.*

María Fernanda Rodríguez, presidenta de ISACA capítulo Quito-Ecuador promueve la actualización profesional y el establecimiento de redes de profesionales afines. La ejecutiva tiene bajo su responsabilidad la planificación y supervisión de auditorías de tecnología, seguridad, procesos y financiera de Telefónica Ecuador.

Iniciativas de control de acceso y monitorización de seguridad

Las empresas ecuatorianas grandes o medianas que miran hacia los negocios digitales cuentan con iniciativas de seguridad relacionadas con el control de acceso a información e implementación de soluciones que permite gestionar la seguridad.

María Fernanda Rodríguez, presidenta de ISACA capítulo Quito, señala que el control de acceso, así como la gestión de identidad y la configuración de seguridad en infraestructura tecnológica, constituyen las primeras líneas de acción en que se encuentran trabajando las empresas ecuatorianas, aunque señala que, si no existe una conciencia y compromiso de la alta dirección con la seguridad de la información, este tipo de soluciones resultarían poco efectivas frente a un evento de seguridad.

Las empresas medianas y grandes en el país trabajan en:

- Control de accesos y actividades
- Implementación de parámetros de seguridad: base de datos, sistemas operativos, seguridad perimetral.
- Monitorización de Seguridad

La clave antes de implementar soluciones de seguridad es ser consciente de la información de la organización y de las transacciones más sensibles.

De nada sirve el monitoreo de logs, o trabajar en el monitoreo de actividades si no existen procesos adecuados que permitan saber cuáles son las transacciones sensibles sobre las que se debe emprender acciones de auditoria conjunta, configurar alarmas o elementos correlacionados para analizar comportamientos y trasladar al equipo de monitoreo procedimientos inusuales que se convierten en amenazas para prevenirlas o recuperarse si algún ataque se materializa.

En un negocio digital donde las áreas comerciales sobre todo, tienden a desarrollar iniciativas digitales es necesario generar un mix de capacidades del encargado de seguridad, tanto desde lo tecnológico como de la visión funcional comercial para concientizar a las áreas comerciales y del negocio que en lo digital existe una mayor exposición. El especialista debe transmitir esa cultura y comunicarse con profesionales afines para madurar los niveles de seguridad y proveer de facilidades y transaccionalidad a los usuarios.



el escenario del **negocio digital**

Un profesional proactivo en seguridad

Los encargados de seguridad de las organizaciones deben trabajar en romper paradigmas locales que señalan que un negocio digital puede ser inseguro para los usuarios.

Más allá de reconocer que los usuarios son una de las amenaza más grandes para la seguridad de la información debido a su papel activo en generar, procesar, almacenar y transmitir información, también es necesario destacar el rol de los profesionales de seguridad.

Éstos profesionales a cargo del área de seguridad de la información toman un rol más proactivo y desarrollan iniciativas en función de una oportuna evaluación de los riesgos inherentes al negocio digital. José Adrián Pino, jefe de Seguridad de la Información de Pronaca, señala que básicamente se adoptan buenas prácticas, sin embargo, hay que considerar que no porque una buena práctica ha dado resultado hay que implementarla sin adaptarla a la realidad de cada organización.

Las empresas ecuatorianas se preparan para ir al negocio digital y cuentan con planes de negocio e inversiones para entregar bienes y servicios a través de canales digitales, de manera que el área de seguridad de la información debe garantizar el acompañamiento para el éxito del negocio, con un adecuado tratamiento de riesgos.

¿Cómo se logra? Para el jefe de seguridad de la información de Pronaca, el profesional de seguridad cumple un nuevo rol que implica el conocimiento del negocio, su proyección, objetivos estratégicos, los productos y/o servicios que comercializa, el marco regulatorio aplicable, las partes interesadas, los procesos core de negocio y demás variables que, con la participación activa de los dueños de los procesos, le permitan identificar los activos de información para el negocio (sin limitarse únicamente a hardware y software), así como las amenazas y vulnerabilidades asociadas a ellos; todo esto, a fin de evaluar riesgos de seguridad de la información y establecer medidas de tratamiento adecuadas para la organización, logrando un marco de control normativo que sea aplicable tanto operativa como tecnológicamente, y sobre todo, que sean interpretados y aplicados por los usuarios, para lo cual se requiere cierto nivel de concientización y una constante mejora continua en cuanto a la gestión y operación de la seguridad de la información.

Nuevo rol del profesional de seguridad

- Ser proactivo.
- Conocer el negocio.
- Identificar activos de información para el negocio.
- Definir qué se debe proteger
- Actuar como capacitadores para transmitir la cultura de seguridad de la información a usuarios finales.
- Implementar controles adecuados.



Adrián Pino, Chief Information Security Officer,CISO de Pronaca.

José Adrián Pino es el Chief Information Security Officer, CISO de Pronaca; además se desempeña como Director de Educación en ISACA capítulo Quito-Ecuador. Es ingeniero en sistemas de la Universidad Internacional SEK, cuenta con Maestría en Gerencia de Sistemas en la Universidad de las Américas (UDLA).

Protección de la información con enfoque de negocio



Roberth Chávez, gerente Senior de Asesoría de Riesgos en Deloitte Ecuador.

Roberth Chávez, es Gerente Senior de Asesoría de Riesgos en Deloitte Ecuador se especializa en servicios de Ciber-seguridad. Ejerce la docencia en programas de Maestría en Auditoría de TI de la UEES y de la Maestría en Sistemas de Información Mención Seguridad de la Información de la UTE. Ha participado en varios proyectos para cubrir los requerimientos del Acuerdo No. 166 de la SNAP en entidades públicas, y JB-2012-2148 y JB-2014-3066 para entidades del sistema financiero nacional.

El desarrollo de estrategias de seguridad para un negocio digital comprende tres aristas fundamentales: personas, procesos y tecnología. Las empresas ecuatorianas tienen comportamientos variados en relación a la seguridad de la información. Roberth Chávez, gerente Senior de Asesoría de Riesgos en Deloitte Ecuador, enumera tres tipos de empresas: las reactivas en asuntos de seguridad de la información, aquellas que se remiten a implementar soluciones tecnológicas, y un tercer grupo de empresas que emplean estrategias para optimizar la gestión de seguridad.

Es sencillo identificar a través de concepto de Pareto el nivel de prioridades de la seguridad, es decir identificamos el 20% de la información que genera beneficios en la organización y que posibilita la operatividad en un 80% de la organización. "Si me ocupo de ese 20%, aseguro la continuidad del 80%", menciona Chávez.

La seguridad de la información debe ser concebida con una visión estratégica y de negocio, caso contrario será vista como un gasto y no como una herramienta habilitadora de negocio, servicios y procesos más seguros. Las empresas deben encontrar el balance adecuado entre protección de información y desarrollo de negocio y en esa tarea el profesional de seguridad debe actuar frente a una audiencia no técnica como el área legal por ejemplo y transmitir su mensaje en términos de negocio.

El encargado de seguridad cumple facetas técnicas como: implementar soluciones tecnológicas y monitorear los resultados de dichas herramientas, pero además, convertirse en consejero para influenciar sobre la importancia de tomar en cuenta los riesgos de seguridad cuando se introducen cambios en la estrategia empresarial y finalmente, alinear la estrategia de seguridad con la del negocio.

El encargado de seguridad debe ganar apoyo ejecutivo y para ello es necesario:

- Conocer el negocio.
- Evangelizar a la alta dirección.
- Llegar con mensajes claros.
- Hablar con el lenguaje del negocio.

La seguridad en el **entorno digital**

Una era hiperconectada a través de conexiones con dispositivos móviles o fijos, las facilidades para transaccionar gracias a distintas plataformas móviles, la transformación digital son escenarios que poco a poco se vuelven comunes en las organizaciones. En ese entorno digital son distintas las acciones que se pueden emprender frente a posibles riesgos.

MDM para dispositivos móviles



► Denise Giusto, investigadora de Seguridad en ESET Latinoamérica.

Los dispositivos móviles se añade al resto de sistemas dentro de una estrategia de seguridad en la organización y más aún cuando las empresas facilitan a sus colaboradores conectarse y trabajar desde sus dispositivos, dice Denise Giusto, investigadora de Seguridad en ESET Latinoamérica, durante el Eset Day.

Las compañías pueden emplear herramientas como Mobile Device Management, MDM, para proteger los mensajes de SMS o códigos maliciosos como randsomware en los dispositivos móviles. Pero también hay que generar políticas de seguridad y gestión de aplicaciones instaladas, dice Giusto.

Los ataques en celulares generalmente son a través de aplicaciones móviles para distintas plataformas por ello, se recomienda diseñarlas bajo un esquema de desarrollo seguro en cada plataforma.

La seguridad en la transformación digital

La transformación digital es inevitable y la seguridad es una pieza fundamental para lograr un balance adecuado entre operatividad y control que permita a la compañía actuar en un entorno de acuerdo a su "tono de riesgo", señala Diego Oviedo Frasson, Associate Partner IBM Security.

En este proceso de transformación, los usuarios deben asumir cambios, de manera que la experiencia del usuario es fundamental, por ejemplo, hacer la inscripción sencilla pero a la vez segura. En la medida en que el negocio conozca sus riesgos podrá tomar mejores decisiones incentivando la transformación digital con un riesgo controlado.



► Diego Oviedo Frasson, Associate Partner IBM Security.



► Carlos Bolívar, gerente Regional para Soluciones Avanzadas de Cisco.

El correo electrónico es un vector de ataque

Para Carlos Bolívar, gerente Regional para Soluciones Avanzadas de Cisco, el vector de ataque principal es a través del correo electrónico y del uso de archivos, por lo que es necesario implementar una estrategia de ciber-seguridad que incluya temas tecnológicos y de servicios para protección perimetral, redes internas, cloud, y de herramientas de cumplimiento de confidencialidad que defina la organización para atender los incidentes de manera rápida y efectiva; además, de una campaña de concientización del usuario final.

La transformación digital es una gestión compartida en **Banco D-Miro**

La transformación de Banco D-Miro, empezó hace cinco años, cuando dejó de ser una Fundación durante 20 años y se convirtió en un banco especializado en micro-finanzas con cobertura en la costa ecuatoriana.

Con una cartera de 92 millones de dólares y capital noruego, provee microcréditos a sectores vulnerables y no bancarizados de la población. La proyección del banco hacia la digitalización empezó el año pasado bajo un plan estratégico de negocio basado en tecnología. Lenin Loyola, gerente general de Banco D-Miro, señala "lo que hagamos tecnológicamente en la institución responde a cinco ejes estratégicos: desarrollar la marca en el mercado, mejorar el servicio al cliente, mayor eficiencia y cobertura, así como potenciar el negocio tanto en la emisión de créditos como en la captación bancaria local".



► *Lenin Loyola, gerente general de Banco D-Miro; Miguel Fuentes, gerente de IT de Banco D-Miro.*

Banco D-Miro conserva los principios de Seguridad SD3+C, Seguro por diseño, seguro por predeterminación, seguro por implementación y la comunicación.

En la primera fase de esta transformación se implementará el Software T24 de Temenos, un core bancario que reemplaza al que utilizaba la institución. Miguel Fuentes, gerente de Tecnología y Procesos, menciona que el core bancario cubrirá sus necesidades para proyectarse hacia una banca digital, la creación de nuevos productos y la reducción de costos operativos. "Las características de T24 nos permitirá incorporar canales electrónicos, la aplicación de conceptos de ATM propios, efectivo móvil, y adoptar el uso de teléfonos inteligentes con acceso a través de conectividad o uso de SMS, inclusive diseñar productos B2C para nuestros usuarios".

Los proyectos de la institución para convertirse en una banca digital incluyen puntos de atención a clientes en ATM para retiros, pago de servicios y de crédito; kioskos virtuales, banca en línea y a su vez la creación de agencias virtuales bajo el cumplimiento de normativas y regulaciones; y la incorporación de corresponsalías no bancarias para ampliar la cobertura.

Bajo la premisa de que en microfinanzas es vital que el banco vaya al cliente, la institución desarrolla herramientas para reforzar la parte operativa. Loyola explica que el eje de acción serán las microfinanzas con la entrega de créditos para microempresarios; pero también se abrirán hacia la captación de esos mismos microempresarios como nuevos nichos del mercado financiero.

En este proceso de transformación la gerencia general y gerencia de tecnología tienen varios retos. Entre ellos, lograr el retorno de la inversión y la seguridad. "En un negocio digital existe una mayor exposición a ataques que vulneren las seguridades, de manera que es necesario, implementar y cumplir altos estándares de seguridad para la provisión de nuevos productos y servicios, señala Miguel Fuentes.

El plan de seguridad está basado en las mejores prácticas de los estándares ISO 27000, política de seguridad interna, cumplimiento normativo como la norma 3066, donde se analizan las seguridades externas e internas y conceptos de privacidad y confidencialidad siguiendo las normativas para el sector.

Miguel Fuentes, gerente de IT de Banco D-Miro, enfatiza que el trabajo en conjunto permite alinear tecnología con el negocio, de manera que cualquier inversión que realice IT, cumpla con los objetivos de la estrategia de negocio de manera que "no se tecnifique el caos". Y en esa línea de acción están abiertos a las fintech que tienen ideas innovadoras pero bajo un análisis detallado no solo de la tecnología con que cuenta la organización, sino también, de servicios, productos, necesidades y requerimientos de los clientes.

Omnicanalidad e innovación en la mira del **Banco del Pacífico**

El Banco del Pacífico es la segunda institución más importante de la banca en el país. En febrero del 2017, el banco registró en el Estado de Situación Consolidado y Condensado de la Superintendencia de Bancos, un total de pasivos, patrimonio e ingresos por un valor de USD. 5.242.963,10.

Durante 45 años, Banco del Pacífico ha evolucionado hacia un modelo de negocio digital implementando canales electrónicos y digitales para sus clientes. Uno de sus más recientes, es Smart Pacifico, una aplicación móvil dirigida a clientes de 18 a 25 años, a través de la cual se puede abrir una cuenta y realizar transacciones digitalmente.

La institución bancaria tiene planes de innovación con la creación de nuevos productos y servicios bajo el modelo de omnicanalidad donde la experiencia del usuario sea la misma a través de todos los canales a los que tiene acceso el cliente.

José Luis Nath, gerente Nacional de Seguridad Bancaria del Banco del Pacífico, menciona que la omnicanalidad desde el punto de vista de seguridad debe ser entendida como una "única experiencia", debe ser amigable, confiable y adaptable e ir de la mano con la promesa de venta y operativa.

La innovación de productos y servicios de la institución bancaria gira en función de la omnicanalidad y seguridad, de manera que "estamos diseñando y creando productos innovadores donde la parte de seguridad no sea un tema restrictivo sino facilitadora del negocio", indica el ejecutivo.

Las instituciones financieras tienen que asegurar los nuevos modelos digitales, y las transacciones de los clientes, con esta visión la creación de productos en el Banco se ajustan a las normativas establecidas 2148, y 3066 de la Junta Bancaria. Un sistema de protección integral basado en mecanismos robustos y de doble autenticación, así como programas de capacitación para los clientes sobre el uso de canales electrónicos.

La banca móvil, Movilmático, de la institución tiene implementado biometría facial, un sistema de reconocimiento del rostro que identifica automáticamente la imagen digital autorizada y registrada por el cliente. "Estamos en un ciclo de aprendizaje donde el cliente acoge y adopta esta tecnología y a medida que madure continuaremos utilizándola en beneficio de las necesidades de los nuevos clientes".

La banca está experimentando una transformación y es importante cambiar la forma en que hacemos las cosas, dice Nath, "las nuevas exigencias de seguridad en el negocio digital deben reducir al máximo el impacto en la experiencia del cliente, y la adaptación de nuevas tecnologías de seguridad deben generar valor en la organización y desechar el paradigma de que "aplicar seguridades" es una limitante del negocio.



► José Luis Nath, gerente Nacional de Seguridad Bancaria del Banco del Pacífico.

Para José Luis Nath, gerente Nacional de Seguridad Bancaria del Banco del Pacífico, los líderes de IT frente a las nuevas exigencias de los negocios deben:

- *Tener clara la existencia de amenazas y establecer las medidas de seguridad tratando de reducir al máximo el impacto en la experiencia del cliente.*
- *Adoptar nuevas tecnologías de seguridad para negocios digitales e incorporarlas en los flujos de negocio como "drivers" o generadores de valor y romper el paradigma de que "aplicar seguridades" es una "limitante de negocios".*

Banco ProCredit, busca mejorar la experiencia de sus clientes

El Banco ProCredit Ecuador es uno de los 14 bancos pertenecientes al grupo ProCredit de Alemania. En el país, la institución con 40 mil clientes a nivel nacional, busca un modelo de transformación que combine los requerimientos del negocio y la infraestructura tecnológica.

Desde hace un año, Banco ProCredit está en un proceso de aceleración hacia la transformación digital y ha considerado por un lado, la implementación tecnológica para acercar los servicios al cliente, pero además, incorporó el concepto de oficinas que operan sin efectivo, oficinas Cashless.



► *José Hernández, jefe de IT de Banco ProCredit.*

En Banco ProCredit, los temas y proyectos que afectan o benefician a los clientes se discuten a través de los comités de tecnología, IT es un área fundamental en la institución para alcanzar los objetivos estratégicos.

Al momento, existen tres oficinas de este tipo en las ciudades de Quito, Guayaquil y Otavalo y son centros de interacción personalizada de negocios, es decir para la captación de nuevos clientes.

Para Miguel Ebenberger, gerente General de Banco ProCredit, la meta trazada es transformar el negocio para sus actuales clientes y brindarles la mejor experiencia de usuario a través de una plataforma digital de interacción de servicios.

En esa medida, prevén una oferta de canales y servicios para los clientes bajo la modalidad de "selfservice", con tarifas atractivas, comodidad, rapidez, y acceso para sus clientes privados, de medianas y pequeñas empresas. Mientras más clientes puedan obtener servicios en el mundo digital, indica José Hernández, jefe de IT de Banco ProCredit, más eficiente será el servicio y menores los costos asociados a estos.

En Banco ProCredit, por ejemplo, se maneja un modelo de negocio al cual los clientes pueden acceder a todos los servicios bancarios al momento de abrir su cuenta corriente transaccional, operaciones como transferencias nacionales, internacionales, compras en línea mediante su tarjeta de débito, uso de tokens, consultas en línea o mediante Banca telefónica son parte de este modelo.

Los retos frente a los nuevos modelos digitales en la banca se dan en dos frentes, por un lado, está la seguridad, pues los clientes comparten información crítica y sensible; y de otro lado, la gestión de IT para alinear de manera total el negocio con la dirección y visión del negocio. Para ello, dice Hernández, se debe concientizar en los distintos niveles de la organización sobre cuál es el futuro que se prevé alcanzar con la transformación digital.

La seguridad tiene que abordar mecanismos que den confianza a los clientes. Banco ProCredit tiene un marco de gobierno corporativo que incluye políticas de gestión de riesgo tecnológico a nivel del grupo y estándares altos sujetos a los organismos de regulación bancaria alemana y las normativas ecuatorianas, menciona Miguel Ebenberger.

Además, en la institución se han jerarquizado los niveles de seguridad en siete capas que involucra a personas, procesos e infraestructura. José Hernández, dice "hablamos de seguridades físicas, políticas robustas de seguridad de la información sujeta a regulación local y a estándares internacionales que permita la disponibilidad, accesibilidad e integridad de la información. Además, seguridad perimetral de redes y sistemas; vulnerabilidades, control robusto de acceso y un plan de continuidad del negocio actualizado que se complementa con monitoreo y concientización a los usuarios".

En el proceso hacia la transformación, Miguel Ebenberger, gerente General de ProCredit aspira a que en el plazo de dos años, la mayoría de clientes, un 95% operarán a través de la plataforma digital con personal calificado por encima del promedio de la banca, y que provea asesoría al cliente en temas de valor agregado.

Además, la apertura de nuevas agencias no transaccionales para hacer negocio.



Amenazas en la era digital

Por: David López
Director de Ventas para Latam
de Easy Solutions

En la era de los negocios digitales, las organizaciones, entidades, estatales, aerolíneas, cadenas de retail y muchas otras han sido víctimas y también son el blanco del cibercrimen. El fraude electrónico ha evolucionado de la mano de la industria tecnológica, y de los milenials, la primera generación permanentemente conectada a sus dispositivos que lideran la revolución digital. Desafortunadamente, aún hay empresas que no son conscientes de la realidad y de estos cambios y no toman la protección adecuada para prevenir amenazas y ataques.

Según cifras del Reporte Anual de Seguridad Cibernética de Cisco 2017, más de un tercio de las organizaciones que sufrieron un ataque en el 2016 reportaron una pérdida sustancial de clientes, oportunidades e ingresos de más del 20%.

Las amenazas externas afectan a una marca de una forma irreparable. Las más graves se dan cuando los criminales suplantan la identidad de una marca para sustraer información crítica de clientes y usuarios.

Los cibercriminales emplean las más variadas formas de abuso para atacar a las compañías o a sus usuarios finales, pero muchas veces, el daño a una marca se manifiesta con las denuncias realizadas a partir de las publicaciones falsas, en las cuales la compañía no tuvo nada que ver. Sin embargo, cabe mencionar que el no tomar acciones para protegerse contra este tipo de crímenes les asigna algo de la culpa a las entidades involucradas.

La mejor forma de protección contra los diferentes tipos de amenazas es la implementación de una plataforma con diferentes niveles de soluciones contra fraude, para que las amenazas que no sean detenidas por una capa o en una instancia sean detectadas por otra.



► *David López, Director de Ventas para Latam de Easy Solutions.*

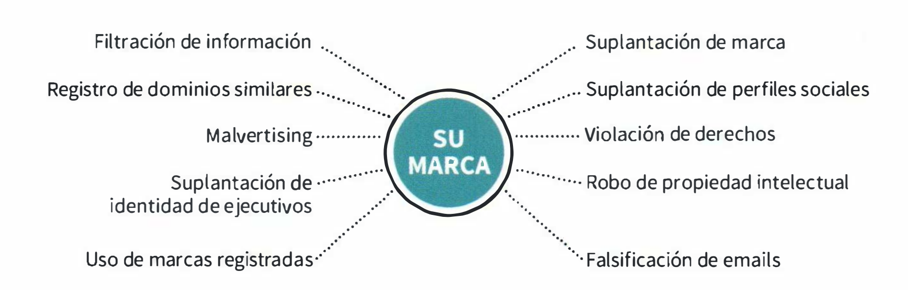
Las empresas y la banca, definitivamente deben contar con un enfoque holístico, multinivel, multicapas; dentro de una estrategia de protección de Amenazas digitales proactiva contra el fraude, mediante la detección y mitigación de ataques diseñados para robar la información personal de clientes y empleados.

Acciones preventivas

1. *Siempre monitoree las plataformas de redes sociales, incluso si su organización no tiene una cuenta en cierta plataforma.*
2. *Encuentre una solución profesional que ofrezca una efectiva detección de phishing.*
3. *Asegúrese de que los cibercriminales no estén utilizando el nombre o logo de su compañía para crear aplicaciones no autorizadas que puedan ser peligrosas.*

Amenazas:

- *Registro de dominios falsos.*
- *Aplicaciones falsas.*
- *Suplantación de emails.*
- *Publicaciones falsas en redes sociales.*
- *Malvertising o uso de la publicidad para ocultar malware.*



Crónica de un ataque: "borrón y cuenta nueva"



► *Miguel Azuero, gerente general Greenbral S.A.*

Hace cuatro años, Greenbral S.A, empresa dedicada a la distribución de productos de consumo masivo para las provincias de Cañar, Azuay y Morona Santiago, perdió toda su información.

La lentitud en el acceso a los sistemas de la compañía, un tráfico anormal en el acceso a información de casi dos semanas, y un correo electrónico que provenía de Australia solicitando cinco mil dólares de rescate por el secuestro de información los alertó tardíamente de que sufrieron un ataque.

Sin acceso a sus sistemas buscaron ayuda, y el diagnóstico concluyó que la información de la organización estaba secuestrada y encriptada. El pedido de rescate fue de 5 mil dólares. Miguel Azuero, gerente general de la compañía con sede en Cuenca, dice que pensó en entregar el dinero, aunque luego de sugerencias no aceptó el chantaje ni realizó el pago, decidió perder la información.

Durante una semana que se paralizaron sus actividades. Se redujeron y suspendieron las ventas no fue posible utilizar el sistema de pedidos móviles del equipo de ventas; a nivel administrativo tampoco se realizó la facturación digital. La compañía maneja alrededor de 8 mil clientes o puntos de venta a los que los vendedores los visitan cada 8 días.

Mientras subían de nuevo la información, trabajaron la facturación de forma manual. Al día emitían 300 facturas y para ello, todo el personal disponible ayudó en la facturación. Con respaldos antiguos de clientes empezamos a construir una nueva base de información. "Fue un borrón y cuenta nueva", dice Azuero.

El gerente de Greenbral S.A, sostiene que la pérdida de este hackeo le costó a la empresa alrededor 30 mil dólares, "hicimos cuenta entre lo que dejamos de facturar, tiempo de horas/hombre que participó en la facturación manual".

Con el incidente se tomaron las medidas correctivas del caso, se definieron políticas de mayor seguridad, contrataron servicios externos de seguridad, disponen de un plan de contingencia, realizan backup de manera más esquemática y también cuentan con un respaldo en la nube.

Una de las acciones que se tomaron en Greenbral S.A a nivel legal fue denunciar el robo y secuestro de información que sufrieron, sin embargo, en aquella época en las instancias judiciales no sabían cómo proceder, ya que como indica Azuero, no había ni siquiera tipificación de este delito en la fiscalía. Aunque fue presentada la denuncia, todavía este caso no tiene sentencia.

Acciones legales contra el ciber-crimen

En el caso del robo de información se aplicaría lo dispuesto en el Art. 229 del Código Orgánico Integral Penal, COIP. Si una empresa sufre alguna clase de incidente informático puede hacer la denuncia a la Fiscalía y solicitar el análisis forense de los equipos informáticos afectados, a fin de determinar que lo causó, por ejemplo, establecer qué clase de algoritmo de cifrado fue utilizado y si este se puede revertir. También se podría identificar a los atacantes, y proceder a su procesamiento, indica Santiago Acurio, profesor de Derecho Informático de la Pontificia Universidad Católica del Ecuador.

Sin embargo, debido a que el ciber-crimen es transnacional y rebasa fronteras es importante que nuestro país como otros, firmen el convenio de cibercrimen por ejemplo, con la comunidad europea, de esta manera se asegurará la cooperación 24/7 entre los diferentes países que lo han firmado; además, otros acuerdos internacionales de cooperación sobre el uso de la nube con fines contrarios al respeto de los derechos humanos, como señala el convenio mundial de sociedad de la información de las Naciones Unidas.

El CIO debe influir en el directorio

Juan Carlos López
CISA, CISM, CGEIT, CRISC, PMP
CEO Exacta Consulting & Training
COBIT 5 Certified Assessor
COBIT 5 Implementer
jclopez@exacta.com.ec



Para que las inversiones de tecnología e implementaciones críticas como un Sistema de Gestión de Seguridad de la Información, SGSI, generen valor en una organización se requiere de la participación del CIO, pero también de otras funciones críticas que cumplen un papel relevante. Revisaremos, los roles del Directorio y del CEO y como el CIO puede influir para que estas responsabilidades se cumplan.



► *Juan Carlos López.*

El enfoque tecnológico comienza en el Directorio

El Directorio debe asegurarse que en la organización exista un sistema de Gobierno Empresarial de Tecnología, GETI, que se lo debe llevar de la siguiente manera:

- *Evaluando y definiendo cuales son las prioridades de la organización relacionadas a la generación de valor a las partes interesadas a través de la tecnología. La creación de valor se debe traducir en términos de obtención de beneficios, gestión de riesgos y optimización de recursos a través de la tecnología.*
- *Orientando a la organización respecto de estas prioridades mediante principios y políticas.*
- *Supervisando que esta orientación no se quede en el papel y se implementen en la práctica dentro de la organización.*

El CEO debe marcar el tono

La Gerencia debe asegurar de que, en toda la organización se implemente una estructura de catalizadores (políticas, procesos, estructuras organizativas, cultura, información, infraestructura, habilidades y competencias) que aseguren que la orientación dada por el Directorio se haga realidad.

El CEO debe asegurarse que se desarrolla y se gestione un plan estratégico de tecnología organizacional con un portafolio de inversiones alineado y justificado por casos de negocio que aseguren la obtención de valor.

El CIO debe influir

El CIO debe identificar estos puntos débiles relacionados con el GETI e influir en la organización, para que tanto el Directorio como el CEO adopten los roles críticos y necesarios para que las iniciativas tecnológicas logren sus objetivos.

En tiempos en donde la transformación digital, la seguridad de la información y la ciberseguridad, entre otras disciplinas influenciadas primariamente por tecnología se han convertido en una prioridad en la agenda de las empresas, el apoyo y liderazgo de la Alta dirección y la Alta Gerencia es crítico para obtener resultados exitosos. El CIO debe influir y concienciar a la organización para que los roles y responsabilidades de un Sistema de GETI sean asumidos y lograr que la tecnología genere un valor estratégico a la organización.

- Este artículo toma como base en las herramientas presentadas por el Marco de Referencia COBIT 5 desarrollado por ISACA, www.isaca.org

Las tendencias en los



Patricio Ramon
Gerente Senior Asesoría de KPMG

Un 90% de los incidentes analizados tienen relación con la seguridad de la información.

La industria de servicios financieros, que tradicionalmente, se la percibía como la de mayor afectación, en realidad no tiene una ubicación estelar.

En la tercera edición del estudio Radar de Riesgo Tecnológico publicado por KPMG, se identifican las tendencias en los riesgos relacionados a TI basado en incidentes sucedidos durante el último año a nivel global y los agrupa en tres categorías: Seguridad (54.3%), Disponibilidad (36.2%) y Calidad de TI (9.5%). **Gráfico 1.**

Para fines del estudio se considera a seguridad con incidentes de pérdida de información, intencional o no, la afectación a la infraestructura de TI, y en disponibilidad se consideran incidentes de no disponibilidad y degradación de servicios de TI.

Las causas que principalmente ocasionan estos incidentes son: hacking, acceso no autorizado y malware, para seguridad; fallos en software y red para la no disponibilidad de servicios de TI.

La norma ISO/IEC 27000: 2014 define a la seguridad de la información como la preservación de la integridad, confidencialidad y disponibilidad de la información, por tanto podemos asumir que un 90% de los incidentes analizados tienen relación con la seguridad de la información, la cual es una cifra alarmante y que debe mostrar la criticidad de no gestionar la seguridad de forma prolija.

Por otro lado, en el estudio se analizan los principales sectores afectados siendo los de mayor afectación los siguientes: Tecnología, Medios y Telecomunicaciones (TMT) 25.0%, Gobierno 22.8%, Manufactura 15.1% y Servicios Financieros 12.1% **Gráfico 2.**

Porcentaje de incidentes por categoría

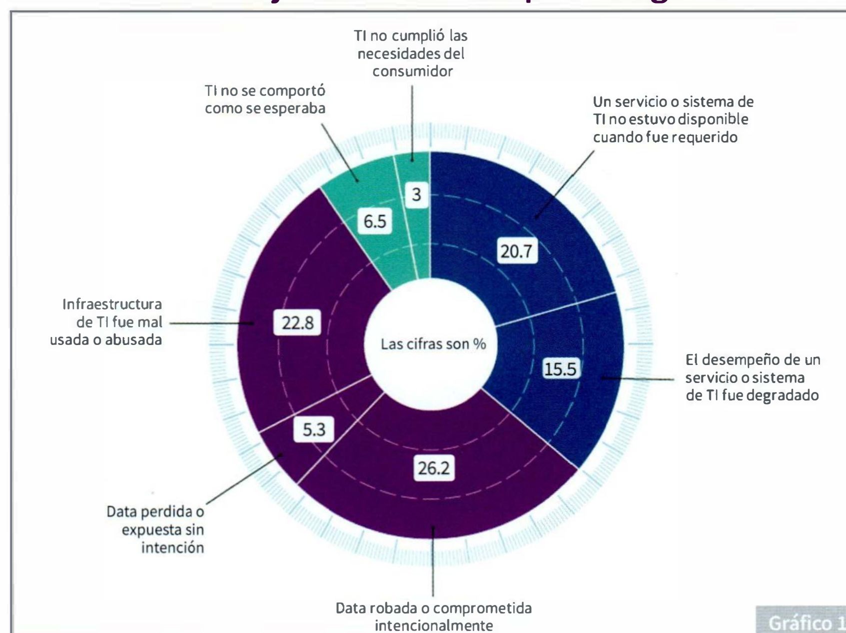


Gráfico 1

De estos datos, se observa que la industria de servicios financieros, que tradicionalmente, se la percibía como la de mayor afectación, en realidad no tiene una ubicación estelar. Y esto se debe, en el caso de Ecuador a las exigencias normativas para administración de riesgo operativo e implementación del estándar PCI-DSS y la madurez alcanzada en el tiempo que hacen que el impacto

riesgos relacionados a TI

de los incidentes de seguridad se haya reducido significativamente.

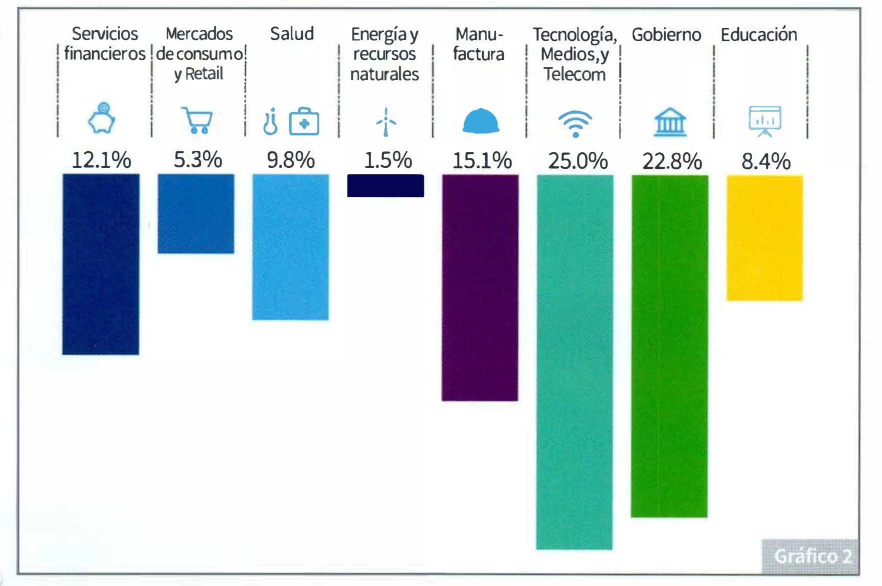
La pregunta que nace es ¿por qué los otros sectores tienen el mayor número de incidentes? Y la respuesta es por la información que manejan. En el mundo digital en el que vivimos, quienes generan valor de la información son quienes lideran los procesos de cambio y están a la vanguardia en innovación, por tanto la información representa un activo de alto valor.

Llama la atención la presencia del sector Manufactura en un tercer lugar, y vemos cómo los cibercriminales han encontrado un nicho importante para delinquir. La capacidad de atacar las redes industriales, las cuáles normalmente no tienen niveles mínimos de protección, más un gobierno de seguridad de la información en su mayoría inmaduro, ha hecho que este sector incremente su presencia en el Radar. Internet de las Cosas está revolucionando los procesos productivos con



Marco Clavijo
Socio de Asesoría de KPMG

Porcentaje de incidentes por Industria



Un enfoque basado en riesgos permitirá a las organizaciones enfocarse en lo significativo, invirtiendo de forma inteligente en las diferentes iniciativas de seguridad de la información.

Este activo es apetecido en un mercado negro que paga por información privilegiada lo que motiva a que los cibercriminales apuesten por incrementar "su inventario" y comercializarlo.

Como hecho destacable, en el año 2013 se emitió el Acuerdo Ministerial Nro. 166 que obliga algunas instituciones del sector público a implementar el Esquema Gubernamental de Seguridad de la Información, el cual es una adaptación de la familia ISO 27001. Este esquema ha creado una línea base de seguridad robusta, la cual irá madurando en el tiempo.

beneficios tangibles, no obstante incrementa la superficie de ataque de las empresas lo que implica que el análisis de riesgo de una empresa de manufactura debe ir más allá del ERP y los procesos que soporta.

Los resultados de este estudio indican que los cibercriminales identifican el valor de los activos de información y la dependencia de TI de las organizaciones para seleccionar sus objetivos, por tanto las organizaciones deben estructurar sus esquemas de protección desde una óptica de riesgos, independiente de su naturaleza, tamaño o ingresos anuales.

Análisis de sentimiento: Seguridad en dispositivos móviles alcanzó mayor interés



► *Juan Pablo Aliaga, Auditor de Sistemas en Corporación GPF.*

La interacción de la información en la nube, será una de las líneas de atención de la ciberdelincuencia.

En colaboración con Machine-Lab e Ingelsi, se realizó el análisis de sentimiento de Twitter, sobre temas de seguridad en cinco categorías: Seguridad en dispositivos móviles, ciberguerra y ciberdefensa, seguridad en la nube, seguridad en Smart grid y seguridad en ciudades inteligentes. Para contrastar lo que dice y piensa las personas en esta red social en relación a las tendencias que se dan en esos temas, Juan Pablo Aliaga, auditor de sistemas y conocedor en materia de seguridad de la información nos hace algunas observaciones.

Sobre los resultados de seguridad en dispositivos móviles, Aliaga, señala que en el análisis de sentimiento se refleja una polarización de opinión hacia finales del 2016, a una aparente neutralidad en mayo del 2017. Esta situación, comenta, tendría su explicación, con el aparecimiento de nuevos riesgos y eventos que afectaron a la seguridad; además, a la percepción de que los dispositivos móviles son el siguiente vector de ataque. Durante, los meses de mayor incidencia emergen con fuerza los conceptos de RoT o "Ransomware de las cosas", donde los dispositivos móviles serían "inutilizados" con el secuestro de información de los mismos.

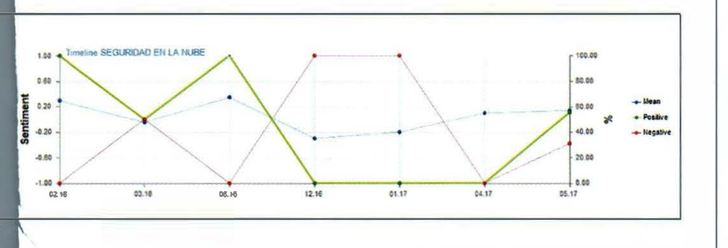
Los resultados de seguridad en la nube se relacionan con eventos sobre filtraciones de seguridad en los meses finales del 2016 y eso repercute de manera negativa en la percepción del público sobre la nube de datos. Aunque, la interacción de la información en la nube, será una de las líneas de atención de la ciberdelincuencia, indica Aliaga.

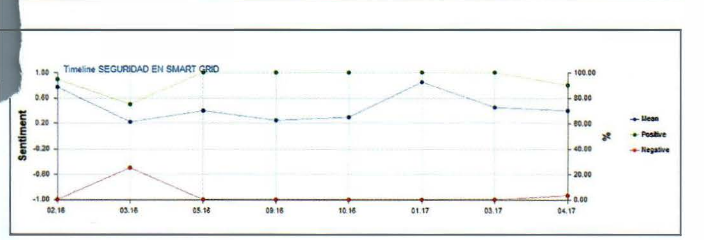
Seguridad en Smartgrid y seguridad en ciudades inteligentes son temas nuevos que aún no tienen un despliegue de información y difusión general, y eso se observa también en las redes sociales como un concepto de "nice to have"(bonito tenerlo), pero que aún no es tangible a pesar del avance de la tecnología a pasos agigantados.

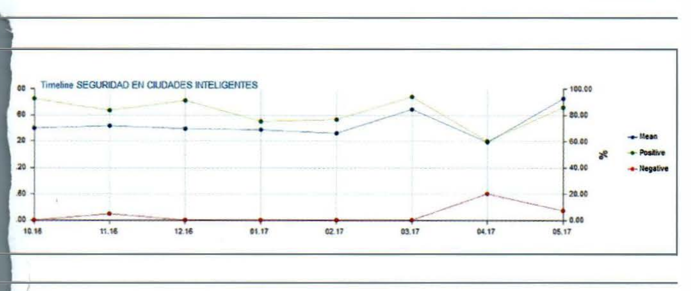
Twitter-Sentiment-Rank ITAHORA

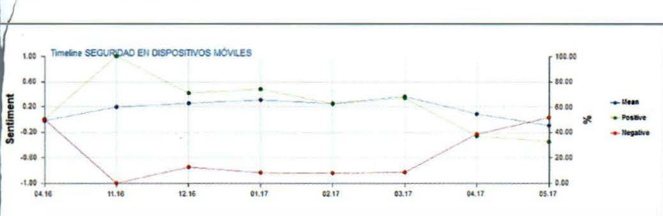
Brand	# Tweets ↓
SEGURIDAD EN DISPOSITIVOS MÓVILES	% 35.95
CIBERGUERRA Y CIBERDEFENSA	% 20.91
SEGURIDAD EN LA NUBE	% 17.60
SEGURIDAD EN SMART GRID	% 13.31
SEGURIDAD EN CIUDADES INTELIGENTES	% 12.23

Los resultados del análisis de sentimiento corresponden de enero de 2016 a mayo de 2017 y se analizaron cuatro categorías generales:













Un proyecto de outsourcing valora costos, seguridad y tiempo



Arturo Salvador, fue vicepresidente de Finanzas y Administración en Toyota del Ecuador,. Actualmente, es gerente Financiero de EP FLOPEC.

Tiene un EMBA y un Diplomado Internacional en Normas Internacionales de Información Financiera NIIFs de la Universidad del Aconcagua de Argentina.

El mayor reto de IT en un proceso de externalización en una organización es demostrar y asegurar que la información de la empresa está segura.

La contratación de servicios de outsourcing o externalización es una de las soluciones que adoptan los directivos, una vez que han considerado los beneficios financieros para la organización. Aunque definir si una empresa está lista o es apta para ello, requiere un análisis previo. Arturo Salvador, con amplia experiencia en finanzas y actual gerente Financiero de la Empresa Pública Flota Petrolera Ecuatoriana EP, FLOPEC, sostiene que es viable que las actividades o funciones que no sean parte del core business sean externalizadas. "Para tomar una decisión de contratación de outsourcing, se debe realizar un proyecto que demuestre que la empresa tendrá mayores ingresos o menos costos sin afectar a los servicios o productos".

En un banco, por ejemplo, debe generar una tasa interna de retorno, TIR, más allá de lo que significaría operar con recursos propios, comenta el experto financiero.

La contratación de outsourcing es un proyecto de la empresa donde se involucran varias áreas y cada una cumple un papel en la adopción y funcionamiento en este proceso económico empresarial. Básicamente, el área funcional donde se realizará la externalización, el área de tecnología y financiera, son las que lideran una vez que el proyecto se desarrolla.

La gerencia técnica define lo que es viable según los lineamientos de seguridad de la organización. El área de IT deberá proteger los datos sensibles para evitar incidentes o fuga de información al compartir datos con la empresa prestadora de servicios; el área financiera ayudará a construir el proyecto, analizará la viabilidad económica del mismo; y finalmente, el área funcional, es decir donde se requiere contratar una actividad bajo esta modalidad.

En esta área se debe analizar las implicaciones sobre los clientes internos y externos según el tipo de externalización, por ejemplo, si una empresa decide externalizar la contabilidad, la afectación directa es sobre el cliente interno; sin embargo, al cliente externo puede afectarle las acciones que se den sobre procesos de servicio al cliente o de venta, menciona Salvador.

El papel del área financiera en el desarrollo de todo el proyecto es analizar previamente y comparativamente en una proyección de 3 a 5 años las implicaciones económicas del proyecto. Lo que el área realiza, dice Salvador, es un cálculo del valor presente, los flujos futuros y los compara con los datos actuales.

Por ejemplo, si una empresa define que las actividades de nómina o rol de pagos lo realizará una empresa externa, se analiza la infraestructura física asignada por la empresa, es decir el número de colaboradores que trabajan en esta actividad, además, otros costos por suministros, equipos tecnológicos, licencias del software que utilizan, remuneraciones de los colaboradores que realizan el proceso de nómina. Estos valores, que representan el pago por mantenimiento de la estructura actual, se ajustan anualmente.

El beneficio económico para la empresa, se determina preparando los flujos de caja futuros para la estructura actual y los flujos proyectados para el caso de outsourcing, señala Salvador.

Viabilidad de outsourcing o externalización desde el punto de vista financiero

FLUJO DE CAJA						
Proyección de flujos de caja **En miles de US Dólares**	**Años** **0**	**1**	**2**	**3**	**4**	**5**
A) Flujo proyectado con estructura actual *						
Cobros por ventas (ingreso de caja)		917	1.183	1.429	1.771	1.983
Pagos estructura actual (salidas de caja)		-756	-902	-1.045	-1.263	-1.510
Flujo de caja sin descuento	**0**	**161**	**281**	**384**	**508**	**473**
Tasa de descuento	12%					
Valor actual neto	**1.232**					
B) Situación proyectada con Outsourcing**						
Costos Outsourcing	-424	-227	-249	-278	-332	-393
Cobros - ingresos de caja		917	1183	1429	1771	1983
Pagos estructura modificada		-303	-431	-490	-591	-690
Flujo de caja sin descuento	**-424**	**387**	**503**	**661**	**848**	**961**
Tasa de descuento	12%					
Valor actual neto	**1.877**					

*En el flujo de caja proyectado con estructura actual, se consideran las salidas de caja (costos y gastos) tal cual opera la empresa, en el año cero no hay ninguna inversión (salida de caja inicial del proyecto).

**En el flujo de caja proyectado con outsourcing, existe un costo inicial por los cambios de estructura que se dan, el mismo que debería generar ahorros en los pagos futuros y eventualmente incrementos en los ingresos.

El resultados es que el valor actual neto de la situación proyectada con outsourcing es mayor al que hubiera generado si mantiene la estructura actual. En este ejemplo, se recomendaría desde el punto de vista financiero realizar el outsourcing,.

Los pasos a seguir previos contratación de servicios de externalización son los mismos que se aplican en todo proceso de compras. Algunos puntos a considerar

- *Definir al detalle las necesidades de la empresa.*
- *Considerar los costos iniciales de un proyecto de externalización.*
- *Estas seguro de los costos de implementación del proyecto.*
- *El tiempo en el cuál se ejecutará el proyecto*
- *Análisis financiero.*
- *Toma de decisión.*

Reingeniería de impresión
permite disminuir gastos



► *Gloria Sandoval, gerente de TIC's de Industrias Ales.*

La externalización representa para la empresa beneficios económicos que para final del año 2017 se estiman entre 25 y 30 mil dólares de ahorro, en relación a gastos respecto al año anterior.

La contratación de servicios, principalmente en época de crisis, es una estrategia que las empresas utilizan para disminuir costos. Las posibilidades que brinda esta modalidad son amplias y los servicios pueden ser contratados para cualquier área del negocio.

En industrias Ales, compañía agroindustrial ecuatoriana, bajo la dirección del área de Tecnologías de Información y comunicación (TIC´s) contrató servicios de outsourcing de impresión. Por medio de un extenso análisis, la empresa decidió contratar los servicios de la empresa Ecuacopia usando sus impresoras RICOH para incorporar centros de copiado en el edificio matriz de Industrias Ales tanto de Quito como de Guayaquil.

De esta manera, centralizaron puntos importantes para generar más eficiencia y eficacia en los procesos.

Gloria Sandoval, gerente de TIC´s de Industriales Ales, junto con su equipo de trabajo, adoptó este mecanismo que representa beneficios económicos para la compañía. Se estima que para el final del año 2017 se ahorre entre 25 y 30 mil dólares en relación a gastos, respecto del año anterior. Los ahorros se evidencian en el consumo de papel, repuestos y mantenimiento de las impresoras.

Ecuacopia incorporó centros de copiado con 4 impresoras de alto rendimiento para cada ciudad. El pago del servicio se mide por click, es decir que si se imprimen 20 hojas se cobrará 20 clicks. De esta manera, esta modalidad ha generado menor costo de impresión y menor gasto en insumos. Respecto a la seguridad de la información, a cada empleado se le asignó una clave personal que debe ingresar al momento de imprimir su documentación.

Además, de los centros de copiado se logró un valor añadido con la implementación de un módulo de gestión documental. En la primera fase, se centralizó en los centros de copiado la administración de los contratos.

El encargado de impresión, también, digitaliza los contratos y los ubica en un índice que está al alcance del personal autorizado de la compañía. En este índice se incluye la fecha de inicio, vencimiento y responsable del contrato. Además, si este está próximo a vencerse, el sistema emitirá una alerta a la persona responsable del contrato para su seguimiento.

Para comprobar la viabilidad del contrato, el área de IT se basó en una investigación previa. "En algunos casos, personas que no utilizaban mucho la impresora tenían a su alcance impresoras de alto volumen, y en otros sucedía lo contrario, personas que requerían de una mejor impresora contaban con un producto de menor rendimiento", mencionó Sandoval. Es por eso que el área decidió realizar una matriz para reubicar las impresoras.

Industrias Ales continua utilizando las impresoras que disponían antes de la reingeniería, y se las usa en áreas que presentan dificultades de movilización, y por lo tanto, no pueden acercarse al centro de copiado, como por ejemplo, el personal de bodega, envasado o planta de producción.

Tras haber culminado este proceso en la empresa, Gloria Sandoval, sugiere a las organizaciones que identifiquen costos ocultos y evalúen si es posible contratar servicios bajo externalización ya que los beneficios se evidencian al momento de su implementación.

El servicio al cliente es una prioridad para los negocios digitales





► Mayor Diélo Jiménez, jefe de Sistemas Hospital de las Fuerzas Armadas.



► María Eugenia Narváez, gerente de Servicio al Cliente Swissotel Quito.

Durante, el conversatorio El Negocio Digital: Cómo mejorar la experiencia del cliente, organizado por IT ahora, compartimos con CIO de importantes compañías ecuatorianas sobre las buenas prácticas, experiencias, dificultades, que impulsa los negocios desde la gestión de tecnología.

También tuvimos la participación de voceros de Avaya con quienes se pudo matizar la conversación desde la visión del proveedor.

En una dinámica cordial entre colegas de industrias de retail, hotelería, salud, se realizaron importantes observaciones sobre el entorno digital. Mientras sectores dedicados a la distribución y comercialización de productos y bienes se encuentran desarrollando oportunidades de negocio con modelos de e-commerce, canales de pago, diseño de canales de demanda on line, en otros segmentos como el de prestadores de servicios de salud, la preocupación gira en relación a la atención al cliente interno y las facilidades, por ejemplo, en el acceso a conectividad a internet, implementar servicios de diagnóstico digitales y mejores prácticas para la recuperación de pacientes.

La gestión de tecnología para servicios de salud, hotelería, retail es diferente debido a las necesidades puntuales de cada negocio, sin embargo, la estrategia y práctica se centra en la atención, servicio y satisfacción del cliente interno y externo.

Leonardo Martínez, gerente de IT de Quifatex en Ecuador, señala que el área de IT complementa lo que es servicio al cliente entregando facilidades para la operación logística, indicadores de ventas, impulso a acciones comerciales, libertades de acceso tecnológico, inventarios, soporte, etc.

El negocio digital utiliza tecnologías disruptivas que mejoran la experiencia de los clientes. En el sector hotelero por ejemplo, las tecnologías cambiaron los modelos tradicionales de demanda y la forma de conocer a los potenciales clientes. En la actualidad, la última expresión de demanda para alojamiento es a través de la página

el nuevo campo de batalla y reto para las empresas es el servicio al cliente y la apertura de canales que le den al usuario facilidades

web del hotel porque el resto sucede en las redes sociales y en la denominadas OTA que en español se conocen como Agencias de Viaje on line, señala Jimmy Nuñez, director de Tecnologías de la Información y Comunicaciones en Quito-Lindo S.A - Hotel Quito.

En el tema del negocio digital, en salud hay un factor diferenciador generacional, indica Roberto Montenegro, gerente de Tecnología del Hospital Metropolitano, "la visión sobre el uso y acceso a los servicios de salud para una mejor estadía en hospitales y centros de asistencia de salud son importantes pero es diferente según la edad de los usuarios"

Xavier Quintanilla, Territory Manager Ecuador de Avaya, señaló que en el negocio digital, el nuevo campo de batalla y reto para las empresas es el servicio al cliente y la apertura de canales que le den al usuario facilidades que mejoren la experiencia de atención, compra, servicios, etc.

Al hablar de negocios digitales, hay que



Víctor Mier, Paula Andrea Gómez, Moisés Quintana y Xavier Quintanilla, ejecutivos de Avaya.

diferenciarlos según el tipo de actividad. Salud, hoteles y retail son completamente diferentes, menciona Dennis Criollo, gerente General de IT Empresarial, empresa que provee soporte a Grupo Farmaenlace, Etafashion, RM, "Inclusive el retail farmacéutico es diferente al de un supermercado, de manera que es necesario buscar e implementar la tecnología necesaria en función de cada negocio" aclara.

El e-commerce junto a una estrategia de marketing digital permanente favorece la experiencia del cliente interno y externo. Por un lado, el cliente interno en la empresa accede a la data para hacer inteligencia de negocios.



Roberto Montenegro, gerente de Sistemas del Hospital Metropolitano.



Leonardo Martínez, gerente de Tecnología Informática de Quifatex.



Mónica La Fuente, gerente de Sistemas de Farmacid S.A.



Jimmy Núñez, director de IT del Hotel Quito.



Dennis Criollo, gerente General de IT Empresarial.

Conclusiones y retos para llegar al negocio digital

- *Promover un control de acceso a internet en las organizaciones a través de buenas políticas de trabajo.*
- *Ampliar las pasarelas de pago.*
- *Definir mecanismos de acompañamiento para incidir en normativas regulatorias que limitan los proyectos tecnológicos en las organizaciones.*
- *Trabajar en una economía de escala para la entrega de servicios comunes.*
- *Conocer, acompañar y tener campañas permanentes de Marketing Digital.*

Soluciones de colaboración y teletrabajo

La implementación de soluciones colaborativas en las empresas, abren múltiples opciones de interacción en distintas áreas y procesos de las organizaciones pero además, la posibilidad de apoyar tecnológicamente, a normativas como el teletrabajo y el trabajo colaborativo.

Los gerentes de IT de las empresas ecuatorianas Kubiec y Ecuasal comentan sus experiencias y estrategias a través del uso de soluciones colaborativas, redes de comunicación, y el gerente de Talento Humano de Seguros Equinoccial, transmite la experiencia en la implementación del teletrabajo.

Ecuasal mantiene una comunicación efectiva



► *Henry Andrade, gerente de Sistemas de Ecuasal.*

En Ecuasal prevén la evaluación de herramientas de ofimática y otras como: Sharepoint (Paas), Team, Skype Empresarial y Power BI.

Ecuatoriana de Sal y Productos Químicos, Ecuasal, empresa ecuatoriana productora y comercializadora de sal, implementó herramientas colaborativas para agilizar sus labores.

En el año 2013, migró la plataforma de correo a Google Apps for Works, (hoy conocida como G Suite) para mejorar la colaboración entre usuarios mediante las aplicaciones Gmail, Hangouts, Google+, hojas de cálculo, formularios.

Debido a las necesidades del gerente de proyectos de Ecuasal se añadió una nueva herramienta a la organización. Teamwork Projects, es un software basado en web que permite maximizar la productividad de los proyectos y su gestión.

Henry Andrade, gerente de Sistemas, sostuvo que se necesitaba un software para compartir archivos y colaborar internamente y con los proveedores que participan en los diferentes proyectos de la organización.

La implementación de estas herramientas generan el uso eficiente de los recursos y "desde el punto de vista financiero, la suscripción a estas aplicaciones es un OPEX, y a nivel funcional, la empresa obtiene mejores canales y una comunicación oportuna con las diversas áreas de la organización".

"Estas soluciones permiten el uso eficiente del tiempo de los colaboradores, compartir y tener disponibilidad de la información 24/7 y fomentar la escalabilidad ante el crecimiento de nuevos usuarios"

Finalmente, la estrategia que plantea a mediano plazo es implementar soluciones de BI. Según Andrade, en un futuro estas soluciones serán parte del sistema colaborativo, "pues una organización es un sistema con procesos que deben estar comunicados y más cuando se trata de revisar y evaluar el progreso de la estrategia del negocio".

En Ecuasal prevén la evaluación de otras herramientas de ofimática y otras como: Sharepoint (PaaS), Team, Skype Empresarial y Power BI.

Las estrategia "home office" de Kubiec mejora el rendimiento

Kubiec, empresa metalmecánica, luego de un estudio previo implementó una arquitectura para "home office" para la conexión remota de los empleados. Hernán Estrella, jefe de Tecnología, explicó que las conexiones VPN a la red corporativa complicaba el trabajo de los usuarios e influía en la productividad del personal. "La existencia de puertos cerrados en los lugares en que se conectaban los usuarios, falta de credenciales para acceder a los servicios, eran los principales problemas". Con estos antecedentes, "decidimos crear una solución que sea transparente para el usuario", recalca Estrella. En Kubiec se utiliza protocolo HTTP con puertos 443, generando una conexión segura. Para ingresar, el usuario escribe su nombre y contraseña. "Muchos de los empleados creen que están ingresando a una página de internet, cuando en realidad están trabajando por Remote Desktop". "El cambio ha disminuido la inoperancia que generaba el fallo de la VPN", comenta Estrella.



► *Hernán Estrella, jefe de Tecnología de Kubiec.*

"Todas las herramientas que hemos implementado son para que los empleados tengan la seguridad de que pueden trabajar desde cualquier lugar en el que se encuentren"

Esta nueva arquitectura tecnológica fue desarrollada por el área de tecnología, no utiliza software de terceros. Trabajaron a nivel de los servidores físicos, habilitando tarjetas de red en los servidores para que se conecten al firewall en una interfaz distinta, previamente configurada; de esta manera, en el caso de existir un ataque, se minimice el riesgo, ya que este solo representa un puente de ingreso a otra infraestructura.

Esta iniciativa de Home Office de Kubiec empezó en noviembre de 2016 en una reunión con la gerencia general y financiera, tras la emisión del acuerdo ministerial de teletrabajo. La propuesta fue implementar una solución para adoptar la modalidad laboral de teletrabajo entre los empleados. "No querían utilizar VPN, buscaban una solución más familiar para el usuario", menciona Estrella. De esta manera, empezaron a trabajar en infraestructura y en el desarrollo de la arquitectura y, en mayo de 2017 el sistema se liberó. La inversión económica fue mínima para la empresa comparada con herramientas de software propietario, indica Estrella.

Utilizan Windows Server con funcionalidades del firewall, creación de DMZ dedicadas, y a nivel físico habilitación de tarjetas de los host. A nivel de infraestructura los accesos son certificados garantizando la seguridad en la conexión.

Actualmente, en este sistema tienen publicado el ERP y los flujos de trabajo de la empresa. Como reto, se planea integrar los otros aplicativos que son Business Intelligence y el Workspace donde se encuentra el file server.

Soluciones colaborativas

Kubiec interactúa con herramientas colaborativas como Microsoft Office 365 y Skype corporativo. Además, utilizan licencia con WebEx para reuniones corporativas que posibilita al personal estar en línea todo el tiempo. Ahora, los funcionarios de todas las áreas pueden reunirse en salas virtuales, sin necesidad de movilizarse de la empresa.

El teletrabajo combina herramientas, habilidades, procesos



► Héctor Cstillo, director de Recursos Humanos de Seguros Equinoccial.

El teletrabajo no solo es una actividad de recursos humanos, sino de un equipo interdisciplinario en el que está involucrado el área de IT, administración y procesos.

Tras la emisión del Acuerdo Ministerial No. MDT-2016-190, en agosto de 2016, las empresas y empleados tienen nuevas posibilidades de empleo amparadas por leyes y regulaciones del Estado ecuatoriano.

Seguros Equinoccial, compañía ecuatoriana de seguros, desde hace seis años incorporó teletrabajo en la organización basándose en modelos de Estados Unidos y Colombia. Actualmente, cuenta con 20 teletrabajadores que laboran jornadas completas y parciales.

Héctor Castillo, director de Recursos Humanos de Seguros Equinoccial, comenta que la iniciativa fue considerada como un proceso estratégico de la compañía en el 2014. En este año, se desarrolló un modelo interno con procedimientos, políticas, fases y acciones aplicables en la organización al momento de optar por el teletrabajo. Además, en esa etapa, se determinó las características profesionales de los empleados y las posiciones que se adaptan a esta nueva modalidad.

El proceso que siguió la empresa para incorporar el teletrabajo, según Castillo consistió en el análisis del cargo que aplica a esta modalidad, funciones, indicadores tangibles, nivel jerárquico, ubicación, roles, etc. Una vez analizado se determinó si la posición puede ejecutarse en teletrabajo.

En cuanto a los empleados, la empresa definió las habilidades blandas y duras que deben cumplir para aplicar al teletrabajo. Estas deben ser automotivación, disciplina, altos niveles de productividad y conocimiento y agilidad en el uso de herramientas tecnológicas. Castillo subrayó que, no todos pueden aplicar para el teletrabajo, ya que el entorno también influye en el desempeño del trabajador. Por lo tanto, al momento de elegir a los candidatos idóneos se genera una matriz en donde se analizan todas las variables y determina si la persona es o no elegible para optar por modalidad de empleo.

Pero este sistema exige que en la planificación se incluya a una persona experta en el área de salud y seguridad ocupacional para prestar las facilidades en la entrega de todas las herramientas necesarias para el teletrabajador y realice el seguimiento laboral. "La compañía debe proveer de un puesto donde cumpla con todos los requerimientos en temas de salud y seguridad ocupacional en relación al espacio laboral, altura de la silla, luz, niveles de ruido y más", subraya Castillo.

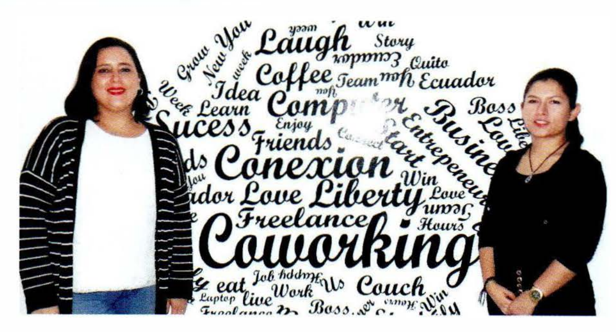
Soluciones colaborativas

En cambio el papel de la tecnología en este proceso es evaluar la conectividad con la que cuenta la persona que trabajará lejos de las instalaciones de la empresa. En el caso de Seguros Equinoccial, Tecnología incorporó soluciones de Microsoft Office, incluyendo Skype for business que permite compartir el escritorio, uso de mensajería con varias personas y generar grupos de trabajo. Adicionalmente, utilizan herramientas de Citrix que permiten la conexión remota a las carpetas de la compañía, así los trabajadores pueden acceder a toda la información de la misma.

La experiencia en Seguros Equinoccial al incorporar la modalidad de teletrabajo significó un aumento entre un 20 y 30% de productividad. "Con el teletrabajo el verdadero retorno de inversión se refleja con la productividad".

Una opción colaborativa para trabajar

Los espacios de co-working resuelven una de las necesidades que tienen los trabajadores remotos que laboran desde sus hogares y es la facilidad de contar con un espacio con los recursos necesarios para realizar reuniones con clientes.



►*Ximena Cabezas y Ángela Vincent, ejecutivas de ConexionEc.*

Estos espacios de trabajo compartido tienen tarifas por horas o meses y varían según el tipo de servicios y facilidades que requiere el usuario. Los costos por hora va desde los tres dólares, y los planes básicos oscilan entre 50 y 70 dólares al mes.

Ángela Vincent, ingeniera en Contabilidad y Auditoría y Ximena Cabezas, ingeniera en Informática, son dos emprendedoras que decidieron abrir un espacio de coworking en la ciudad de Quito. ConexionEC nació luego de que ambas realizaron una investigación sobre espacios coworking y cómo lo manejaban en otros países.

A este lugar acuden profesionales de áreas que decidieron trabajar de manera autónoma. ConexionEC, une a "co-workers" de distintas actividades en un espacio laboral de conocimientos y colaboración, donde además, se realizan talleres y charlas para nuevos emprendedores.

Los espacios de ConexionEC están adecuados para realizar reuniones, tienen acceso a internet, proyector, y otras facilidades como bebidas calientes para los clientes de los coworkers.

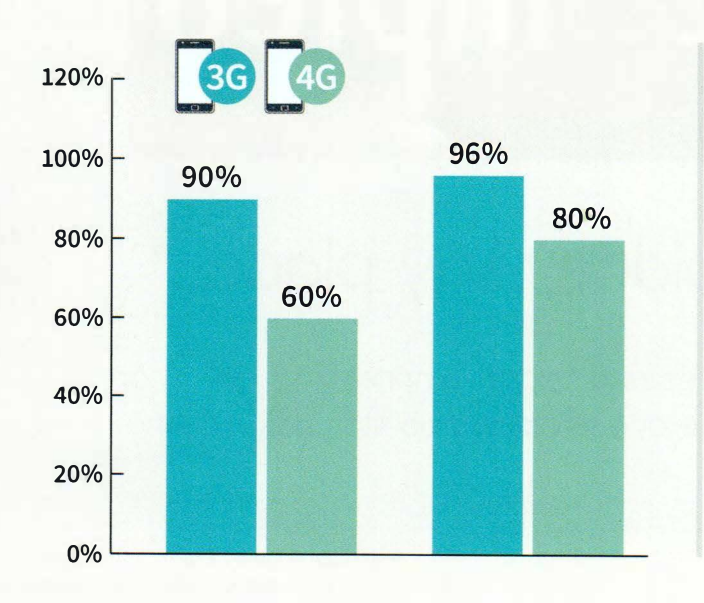
En Quito existen algunos espacios de coworking como Buen Trip Hub, Impaqto, Cowork, Conquito, ConexionEC. Coworking Cuenca es considerado el primer espacio de trabajo compartido que apareció en Ecuador.

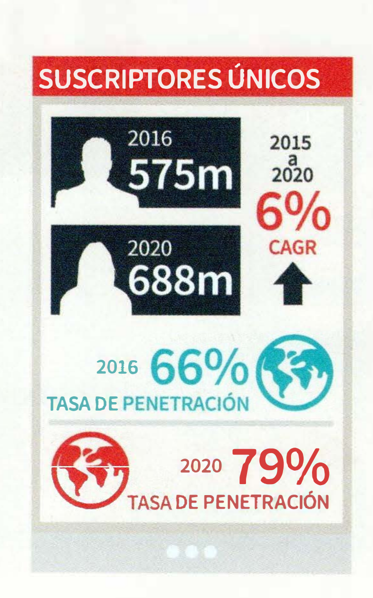
Cifras: mercado móvil, nuevos negocios, transporte

DURANTE EL FORO DE TELECOMUNICACIONES TIC 2017 ORGANIZADO POR SEMINARIUM SE ANALIZARON ASPECTOS REGULATORIOS, CRECIMIENTO DEL MERCADO DE MÓVILES, NUEVOS MODELOS COLABORATIVOS DE NEGOCIO; TENDENCIAS DE IOT, CLOUD, Y SE PRESENTARON CASOS EXITOSOS DE INNOVACIÓN EN SISTEMAS DE PAGOS MÓVILES.











ACELERACIÓN DE LA ADOPCIÓN DE REDES DE BANDA ANCHA MÓVIL Y SMARTPHONES

CONEXIONES DE BANDA ANCHA MÓVIL



2016 60%

2020 79%

SMARTPHONES





Para 2020 habrá 577M de smartphones

Un aumento de 202m desde fines de 2016

NUEVOS NEGOCIOS Y TRANSPORTE

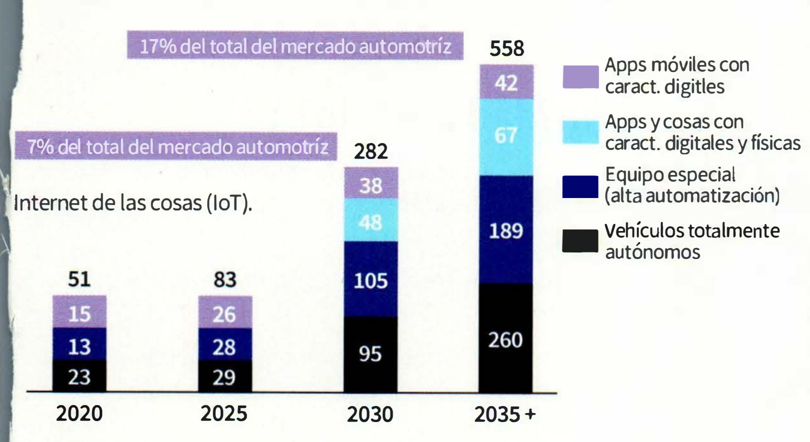
RICARDO WEDER, COO de Cabify se refirió a un reporte de UBS Evidence Lab: Global Automobiles 20 July 2016 donde menciona se han descargado 4 veces aplicaciones de transporte on-demand que autos vendidos en este año, a nivel mundial.

"Las redes deberán estar preparadas para soportar un nuevo panorama de servicios que vendrá con 5G."

Sebastián Cabello, Director general de GSMA para Latinoamérica.

EL VALOR DE LA CONECTIVIDAD MÓVIL

Mercado global de conducción autónoma y automatizada, incluyendo otros servicios (USD. $ Mil millones).



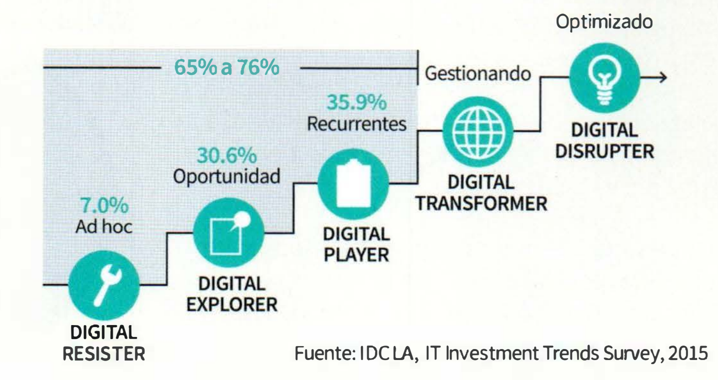
SOBRE TRANSFORMACIÓN DIGITAL

GABRIEL ANDRADA, Director Sector Público y Empresarial Latam de Microsoft, señaló que en el futuro todas las empresas serán empresas digitales. El 86% de los CEOs creen que la tecnología transformará su negocio más que cualquier otra tendencia global en los próximos 5 años

70% de las empresas en Latinoamérica están en etapas tempranas de transformación digital.

Fuente: IDC LA, IT Investment Trends Survey, 2015

70% DE LAS EMPRESAS EN LATINOAMÉRICA ESTÁN EN ETAPAS TEMPRANAS DE TRANSFORMACIÓN DIGITAL



Fuente: IDC LA, IT Investment Trends Survey, 2015

El crecimiento de IoT demanda seguridad



Germán González, CTO & Technical de Colombia y Ecuador de Nokia.

El IoT es una tendencia que se proyecta con un crecimiento vertiginoso. Según Gartner para 2025 habrán alrededor de 25 mil millones de dispositivos conectados a nivel mundial, inclusive empresas como la francesa Sigfox, desarrollan tecnología de bajo consumo de energía y costos como una alternativa para masificar la conectividad de dispositivos pequeños para ser utilizados en distintas empresas o como simples aplicaciones personales en el hogar.

Mientras mayor es la conectividad de dispositivos también crecen los puntos de acceso a la red y los riesgos de seguridad. En las empresas en que se han definido soluciones de IoT se ha gestionado el acceso a la tecnología, sin embargo, no se han analizado aspectos de seguridad. Lo que se busca, dice Germán González, CTO & Technical de Colombia y Ecuador de Nokia, es prestar un servicio pero no existe una preocupación de cómo funciona la estructura del IoT.

González, recomienda que los nuevos emprendimientos y planes de desarrollo deberían contemplar dentro de su trabajo la planeación de aspectos de seguridad y gestión de todos los dispositivos de IoT considerando tiempo, monitoreo, manejo de estándares, pero además la seguridad en la nube, seguridad de los dispositivos de red y seguridad para el monitoreo del tráfico de dispositivos.

Seguridad inteligente para dispositivos

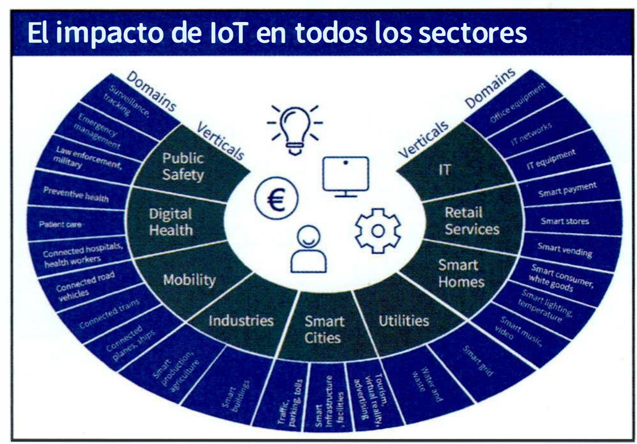
En IoT, las aplicaciones permiten la recopilación y el intercambio de datos para la creación de más servicios. En seguridad física donde se han adaptado sistemas de seguridad electrónica como CCTV, circuitos cerrados de televisión, controles de acceso y presencia, sistemas de intrusión, control de activos, control de acceso gestionado, centros de control de alarmas, etc. éstos dispositivos gracias a la tecnología IP se convierten en inteligentes, y también en un foco que atrae ataques.

González señala que a través de dispositivos de IoT, por ejemplo, de aire acondicionado, es factible entrar a una red en las empresas.

Los ataques más comunes para estos dispositivos son los malware, el Mirai Bot, por ejemplo, cuya acción infecta routers y cámaras IP, escanea los dispositivos enlazados con IoT, accede a credenciales de acceso y carga su código.

La seguridad para IoT :

- *Contar con personal que tenga conocimiento sobre los estándares que se trabajan con IoT para adquirir tecnología cumpliendo especificaciones.*
- *La organización debe tener procesos para la gestión de dispositivo de IoT.*
- *Los operadores como proveedores de servicios utilicen herramientas para mantener seguridades en la red y en sus instalaciones.*



Fuente: Nokia